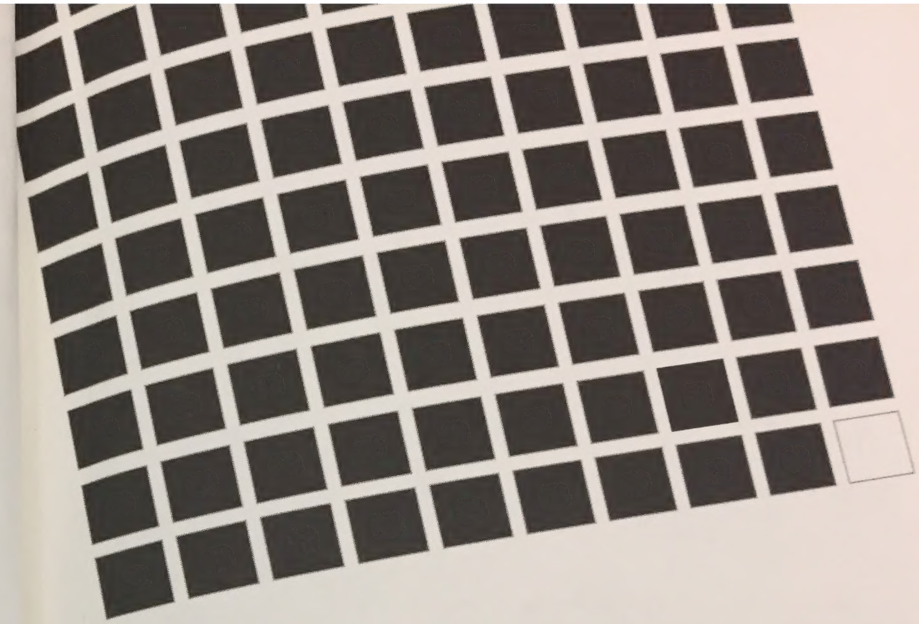
Charles Jennings
and Lori Fena

Foreword by Esther Dyson

The Free Press
New York London Toronto Sydney Singapore



The HUNDREDTH WINDOW

Protecting Your Privacy and Security in the Age of the Interne

Acknowledgments

This book on the great turn-of-the-century Internet privacy and security debate has benefited greatly from many private, off-the-record, conversations with people who shall remain anonymous, ranging from Internet business leaders and technology architects, to strangers on airplanes and dinner party guests. From these conversations, it is clear that few other contemporary issues can evoke such immediate and highly personal concern, or elicit such a wide variety of personal views.

Our public acknowledgment to those who contributed to this book must begin with the volunteer board and hard-working staff of TRUSTe, the Internet privacy assurance organization we founded. Special thanks goes to Gigi Wang and Susan Scott, the original executive directors of TRUSTe, and to Bob Lewin, their successor. They have worked tirelessly to improve privacy practices on the Net, and to develop guidelines for meaningful industry self-regulation. The discussions and debates inside TRUSTe about these guidelines helped us appreciate the complexity of the privacy issue, and the difficulty of finding easy answers to the many questions raised by it.

With respect to the actual research and writing of the book, Russell Shaw made an enormous contribution by providing many of the "Tips and Tricks" found at the end of each chapter, and by helping in other ways too numerous to mention. We could not have finished this book without him.

Much of the research at the heart of this book has been provided to us by Dave Chen and his staff at GeoTrust, an Internet technology company with a special focus on privacy issues. David Garrick, a researcher for GeoTrust, deserves special thanks for his efforts in compiling the "Privacy Incident" log that can be found in Appendix B of this book.

Various friends contributed to our understanding of the technical side of Internet privacy and security—notably, Frank Tycksen of Preview Systems, P. S. Kohli of Intel, Dave Remy of GeoTrust and Pete O'Dell and Michael Hudson of Supertracks. With respect to the development of privacy standards and privacy and security assurance programs, Caroline Buck Luce, Topher Neumann, Geoff Turner and Laura Brown of Ernst & Young's Center for Trust Online have been especially helpful, and supportive. Regarding the rights of individual citizens, or netizens, Executive Director Tara Lemmey and others on the hard-working staff of the Electronic Frontier Foundation have been important contributors—not to just to this book, but to the preservation of basic freedoms in a wired world.

A number of people read early drafts of the book and provided us with invaluable insights, comments, and criticisms. These include: Ron Lunde, Craig Berkman, Lucy Garrick, Dr. Susan Buys, Deborah Robertson, Jan Nichols, Nancy Murray, Nick Nicholas, Dick Luebke, and David and Rebecca Kennerly.

Our editor, Paul Golob, played an essential role in the development of this book. To the extent we have succeeded in communicating complex Internet technology terms and concepts in understandable, mainstream English, he deserves much of the

credit. Heartfelt thanks also to our agents Lynn Chu and Glen Hartley, who helped us turn a personal passion into a marketable book. And to Melissa Hovis, whose organization skills and good sense helped keep our writing on track and on schedule (more or less), and whose personal commitment to the project went well beyond the call of duty.

Finally, we'd like to thank our wonderfully supportive spouses, Christine Jennings and Edward Zyszkowski, who in this case also served as researchers, contributors, editors, critics, and, most important, believers.

computer, and a phone line can obtain instant, low-cost access to highly personal information about us and our families? What will such access mean to businesses, which often collect and use such information, but which have their own privacy and confidentiality concerns as well? What will such pervasive public access to PII mean to government and social institutions? What will it mean to the pursuit of happiness and other quests of the human soul?

We believe that PII levels about each of us will soon approach a kind of critical mass (both in depth of detail and in degree of access), and that the unprecedented public accessibility of private information will generate a considerable hue and cry in response. Consequently, we believe, a tension between the growth and optimization of the Internet, and the growth and optimization of what is uniquely human, will arise and might perhaps produce a dynamic equilibrium, a new solution that can balance the societal demand for technical and economic growth with individual needs for privacy, dignity, and freedom. This book is an exploration of the new Internet privacy and security landscape, in search of this solution.

TRUSTe and Full Disclosure

The Internet privacy and security zone is terrain we know fairly well. Four years ago we founded the Internet privacy assurance organization TRUSTe (www.TRUSTe.org). We have remained active, unpaid volunteers for TRUSTe ever since. Lori still serves on its board of directors, as chairman.

TRUSTe now has over one thousand licensees in its online privacy assurance program. Participating websites agree to post and adhere to privacy policies in exchange for the right to display the TRUSTe seal on their site. TRUSTe does not make judgments about how these licensees collect and use data, so long as they openly disclose their PII practices to site visitors. Disclosure by a website of how it treats private information not only leads to accountability but also builds user trust and confidence. And what's true on the Web is also true in analog media, including books such as this one. And since studies of cross-cultural assimilation have shown that self-disclosure is actually one of the fastest ways to build trust between people, here, then, is a little self-disclosure, from your authors.

Lori is currently chairman of the Electronic Frontier Foundation, a prominent Internet electronic rights advocacy group, and has served on the board of directors of such Internet firms as Critical Path Beatnik, and Urbanite. Charles is founder and CEO of Supertracks, an Internet company that provides services for the distribution of music directly over the Web, and chairman and co-founder of GeoTrust, a provider of systems and services that support trust and transparency on the Net; and co-founder of Preview Systems, a public Internet company. Individually, we have actively supported, through investment or consulting, a number of other Internet companies as well, most of which have been directly or indirectly involved in computer and Internet security issues.

Privacy-loving though we are, no one has ever accused either of us of being shy about expressing our opinions. Here, therefore, are our beginning biases and opinions:

- We are aggressively pro-privacy. We consider respect for individual privacy a bedrock human value. We believe that all users of the Internet need to understand—and have an inherent right to know and control—how information about them is being collected and used.
- We believe that privacy helps keep us free—free, among other things, to make and learn from our own mistakes.
- We recognize that the Internet business community is a uniquely interconnected industry operating in an unusually transparent environment; and feel that the pioneers of this in-

dustry have, f
ethical stand
ity about the
- We believe t
use of PII, a
(fortunately)
of trust will
vacy, and se
of electroni
- We are cert
uses of info
very ones th
mation in
prime exan
- We believe
with respec
and that th
own PII p
addresses,
dossiers th
ment pur
- We believ
enforcing
obvious p
unenforc
- We valu
can, ofte
Alaska o
We beli
part of r

We shoul
this book is n

dustry have, for the most part, operated with surprisingly high ethical standards if perhaps not yet enough care and sensitivity about the confidentiality of private personal information.

- We believe that the business stakes surrounding privacy, the use of PII, and the development of customer trust are huge (fortunately), and that the development of new technologies of trust will be central to the solution of ongoing trust, privacy, and security issues and, indeed, the continued growth of electronic commerce.
- We are certain that some of the most powerful and beneficial uses of information technology in the years ahead will be the very ones that require the greatest amounts of personal information in order to be effective (medical treatments are a prime example, but there are many others).
- We believe that government has a very important role to play with respect to the use of PII for business and other purposes, and that this role begins with leading by example, getting its own PII practices in order and making sure people's names, addresses, auto license plate numbers, and government dossiers that were collected for a specific citizen-to-government purpose don't end up online or resold.
- We believe, further, that government should concentrate on enforcing existing laws well, and tackling very specific and obvious problems, before rushing to pass generic, vague, or unenforceable privacy regulations.
- We value and protect our own personal privacy as best we can, often to the extent of heading into the backwoods of Alaska or Oregon, respectively, without so much as a beeper. We believe that preserving fully private experiences is a vital part of retaining our cultural and environmental heritage.

We should also disclose now, lest there be any confusion, that this book is not intended to be a sober treatise on privacy and pub-

Appendix A

Playing It Safe on the Web: Consumer Dos and Don'ts

Good company-to-customer relationships are built on trust. More and more companies are addressing users' concern about privacy by developing clear internal privacy policies and by posting privacy statements about these policies on their websites. The better companies also get your consent before collecting or sharing personal information. In the end, however, you are the single most powerful protector of your privacy online. It's your voice and your choice that will make the difference.

There are plenty of commonsense rules and take-charge tips for safeguarding your privacy online; TRUSTe has compiled some of the most basic ones (grouped by subject) to help you along. These guidelines are presented below, and together constitute a good summary of solid privacy protection practices for the average Internet user.

Privacy Statements and Seal Programs

Read the posted privacy statements of individual websites to find out what personal information they gather, how it is collected, and with whom it will be shared.

Look for third-party seals, such as the TRUSTe trustmarks. These seals indicate that the website has agreed to submit to third-party oversight and compliance review. In other words, an outside agency checks to make sure that the website actually adheres to its privacy statement. These seals usually link to the privacy statement and to the oversight agency's website.

If you can't find a website's privacy policies, contact the site directly and ask for a copy of its privacy collection and dissemination practices.

Bulletin Boards/Chat Rooms

Be aware that when you provide your name and/or messages to others online through a bulletin board or chat group, they'll probably be able to find out how to communicate with you—whether you want them to or not.

Ward off e-mail messages from strangers by not participating in online chats and bulletin boards. Or consider using a screen name that doesn't directly identify you.

Children

Establish a clear set of online rules for your children. You can always modify or add to the rules as you and your children become more comfortable on the Internet.

Teach your children not to give out their names or other personal information online without your permission—just as they should not talk to strangers! Tell your children to get your permission before responding to online surveys or to games, clubs, or prizes that require personal information for eligibility.

As an added measure of protection, look into purchasing parental control software, which can assist you in supervising online activity when you can't be with your children.

There are software tools that block children from transmitting personal information online, give them Internet access to only those sites predetermined by you or only at certain times of the day, and provide you with a report of the places your children visit online.

Parental control software is inexpensive and easy to install on your computer.

Find out whether your Internet service provider has the technology to restrict children's access to specified sites and prevent online data transactions. A number of commercial online providers have this technology, and all you need to do is request that it be activated.

Cookies

Check to see whether cookie files have been deposited on your computer. If you have a PC, look for a file on your hard drive labeled "cookies.txt" for Netscape browsers and the directory \windows\cookies for IE browsers; look for a file called "magic cookies" if you use a Macintosh. You can remove these files from your hard drive.

If you have a new version of browser software, you may be able to specify that you don't want to receive cookie files or that you wish to be notified when a website is about to deposit a cookie onto your hard drive. Look under the headings Preferences or Options in your software package for such choices, if available.

Credit Reporting Agencies

Periodically request a copy of your credit report, which lists companies that have asked for credit information about you. Call Equifax at 1-800-